Die Hacking Geschichte

Teil 3: Das Computervirus

Bruce Nikkel

Bruce Nikkel Museumsführer
im Museum ENTER

Dies ist Teil drei einer vierteiligen Serie zur Geschichte des Computer-Hacking. In den ersten beiden Artikeln haben wir uns mit dem frühen Hacken globaler Telefonvermittlungssysteme und dem Hacken mit DFÜ-Modems befasst. Dieser Artikel beschreibt die Geschichte des Computervirus.

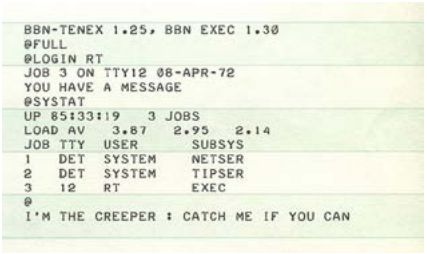
Wir alle haben es satt, über Viren zu lesen, aber dieser Artikel wurde lange vor Beginn der aktuellen Gesundheitskrise geplant. Der Vergleich von biologischen Viren mit bestimmten Arten von Computercode ist auf die Ähnlichkeiten im Verhalten zurückzuführen. Ein Virus verbreitet sich durch verschiedene Kontaktformen, verringert die Funktionalität des infizierten Körpers, verursacht unerwünschte Symptome und kann schwierig zu heilen (zu entfernen) sein.

Sogar die Virenprävention weist Ähnlichkeiten auf, anstelle von Masken haben Computer Firewalls und anstelle von Impfungen verfügen Computer über Antivirensoftware. Die IT-Abteilungen des Unternehmens verwenden sogar das Wort Quarantäne, um die Trennung infizierter Computer von einem Netzwerk «gesunder» Computer zu beschreiben.

Die Verwendung des Wortes «Virus» zur Bezugnahme auf bestimmte Arten von Computercode wurde Mitte der 1980er Jahre von *Fred Cohen* in einem Artikel beschrieben. Ein Wurm ist ein Virus, der sich über ein Netzwerk selbst auf andere Computer repliziert. Ein Trojanisches Pferd bezieht sich auf die griechische Mythologie, in der eine Person etwas (eine Datei oder einen Link) erhält, das harmlos erscheint, aber später bösartigen Code auf ihrem Computer ausführt. Das Wort Malware wurde später als allgemeinerer Begriff für alle schädliche Computersoftware vorgeschlagen.

Andere Beispiele für schädliche oder unfreundliche Software sind Spyware, Adware, Ransomware oder Forkbombs. Die ersten Computerviren wurden von Informatikern, Akademikern und Amateuren entwickelt. Ziel war es, Software zu lernen, zu experimentieren und zu erforschen, die sich selbst replizieren oder bösartig sein kann. Der Virencode wurde als Proof of Concept geschrieben und soll keinen Schaden anrichten.

Eines der ersten Beispiele für ein selbstreplizierendes Programm war der Creeper-Wurm. Es wurde in den frühen 1970er Jahren erstellt und infizierte vernetzte Computer mit dem Betriebssystem TENEX. Der Creeper war harmlos und druckte einfach eine Nachricht mit der Aufschrift «I'M THE CREEPER: CATCH ME IF YOU CAN». Ein Programm namens Reaper wurde später geschrieben, um den Creeper-Code zu löschen.



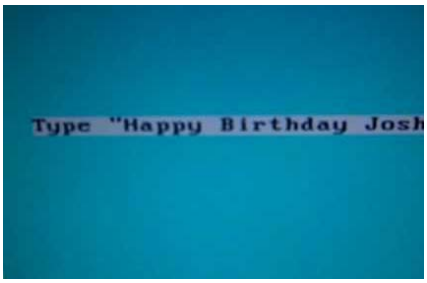
```
BBN-TENEX 1.25, BBN EXEC 1.30
@FULL
@LOGIN RT
JOB 3 ON TTY12 08-APR-72
YOU HAVE A MESSAGE
@SYSTAT
UP 85:33:19   3 JOBS
LOAD AV   3.87   2.95   2.14
JOB TTY  USER      SUBSYS
1   DET  SYSTEM    NETSER
2   DET  SYSTEM    TIPSER
3   12   RT        EXEC
@
I'M THE CREEPER : CATCH ME IF YOU CAN
```

Creeper Worm Output

Einer der ersten Würmer, der weitverbreitete Störungen verursachte, war der Morris-Wurm, der 1988 von dem Studenten *Robert Tappen Morris* geschrieben wurde. Dies war auch der erste Schadcode, der sowohl bei den Nachrichtenmedien als auch bei den Strafverfolgungsbehörden (FBI) grosse Aufmerksamkeit auf sich zog.

Der Morris-Wurm hat eine buffer-overflow Schwachstelle im Finger-Dämon verwendet und die im sendmail-Dämon aktivierte Debug-Funktionalität ausgenutzt. Der Code betraf nur BSD UNIX-Systeme und verbrauchte Ressourcen. Er löschte oder stahl keine Informationen. Innerhalb von 24 Stunden nach seiner Veröffentlichung hatte der Wurm das Internet zum Stillstand gebracht. Dieser Vorfall motivierte die Schaffung von CERTs (Computer Emergency Response Teams) auf der ganzen Welt und war die Geburtsstunde des Bereichs Malware-Analyse und Reverse Engineering, der bis heute aktiv ist.

Mit der zunehmenden Beliebtheit von PCs nahmen auch PC-Viren zu. Ursprünglich wurden die Viren von Leuten geschrieben, die versuchten, lustig oder boshaft zu sein. Diese Viren waren grösstenteils harmlos, im schlimmsten Fall ärgerlich. PC-Viren verbreiten sich normalerweise durch Disketten oder Software, die von BBS-Systemen heruntergeladen wurden (wie in meinem letzten HISTEC-Artikel beschrieben). Wenn die kopierten oder heruntergeladenen Programme ausgeführt wurden, infizierten sie das System. Ein Beispiel war der Joshi-Bootsektor-Virus. Am 5. Januar eines jeden Jahres wurde der Virus aktiv und der Benutzer musste «Happy Birthday Joshi» eingeben, bevor er fortfahren konnte.



Stoned Virus

Der stoned Virus ist ein Beispiel für einen harmlosen, aber ärgerlichen Virus, der den Bootsektor von Festplatten und Disketten infiziert hat. Der stoned Virus wurde bei zufälligen Starts aktiv und hinterliess die Meldung «Ihr PC ist jetzt stoned!». Es gab viele Variationen des Stoned-Virus nach der Originalversion.

Die ersten Virenscanner und Antivirenprogramme wurden mit Mustererkennung erstellt, um Viren zu finden und zu entfernen. Aber Virenschreiber waren sich dessen bewusst und suchten nach Möglichkeiten, um einer Entdeckung zu entgehen. Eine übliche Methode, um eine Erkennung zu vermeiden, bestand darin, die ausführbare Binärdatei dynamisch zu ändern, sodass jeder infizierte Computer eine eindeutige Version zu haben scheint (sogenannte polymorphe Viren). Dies reduzierte die Wahrscheinlichkeit einer Erkennung basierend auf dem Mustervergleich drastisch.

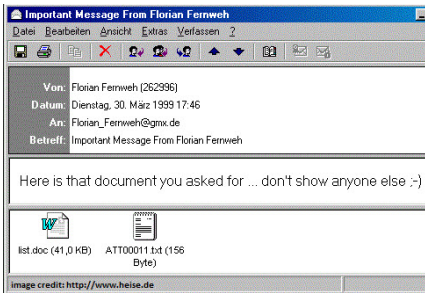
Das Wachstum des Internets veränderte die Verbreitung von Viren. Es war trivial, E-Mails mit böswilligen Anhängen oder Weblinks an böswillige ausführbare Dateien auf Websites zu senden. Personen, die die Anhänge geöffnet oder auf die Links geklickt haben, wurden infiziert. Eine andere Methode der Client-Infektion wird als Drive-by-Infektion bezeichnet, bei der Benutzer im Internet surfen und eine gefährdete Website mit bösartigem Code besuchen, der unabsichtlich auf den PC heruntergeladen wird. Alle diese Methoden werden heute noch verwendet.

Viren betrafen nicht nur Endbenutzer-Clients, sondern auch die Serverinfrastruktur. In den frühen Tagen des Internets waren Server weniger geschützt (keine Firewalls), die Konfiguration war nicht defensiv (unsichere Standardeinstellungen) und Software-Schwachstellen machten es einfach, exponierte Dienste auszunutzen. Ein Beispiel ist der SQL Slammer, der einen Fehler in Microsoft SQL Server ausnutzte und 2003 weit verbreitete Störungen verursachte. Der SQL Slammer ist ein Beispiel für einen Virus, der Denial of Service (DoS) verursacht und das UDP-Protokoll verwendet, um sich so schnell wie möglich selbst zu replizieren.

Als die Leute anfingen, Firewalls und Antivirenprogramme zu verwenden, brauchten Virenschreiber eine neue Methode, um Benutzer zu infizieren. Funktionsreiche Anwendungen und Office-Programme bieten nun erweiterte Skript- und Makrofunktionen, die (zu diesem Zeitpunkt) nicht von Antivirenprogrammen überwacht wurden.

Dies führte zur Entstehung des Makrovirus, der Office-Dokumente infizierte. Ein berühmter Makrovirus, der 1999 gestartet wurde, war Melissa, die MS-Word-Makros verwendete, um sich selbst zu replizieren.

Das Öffnen eines Anhangs mit einem mit Melissa infizierten Word-Dokument, führt dazu, dass Kopien des infizierten Dokuments an die eigenen E-Mail-Kontakte gesendet werden. Diese überlasten E-Mail-Systeme auf der ganzen Welt.



Melissa Virus

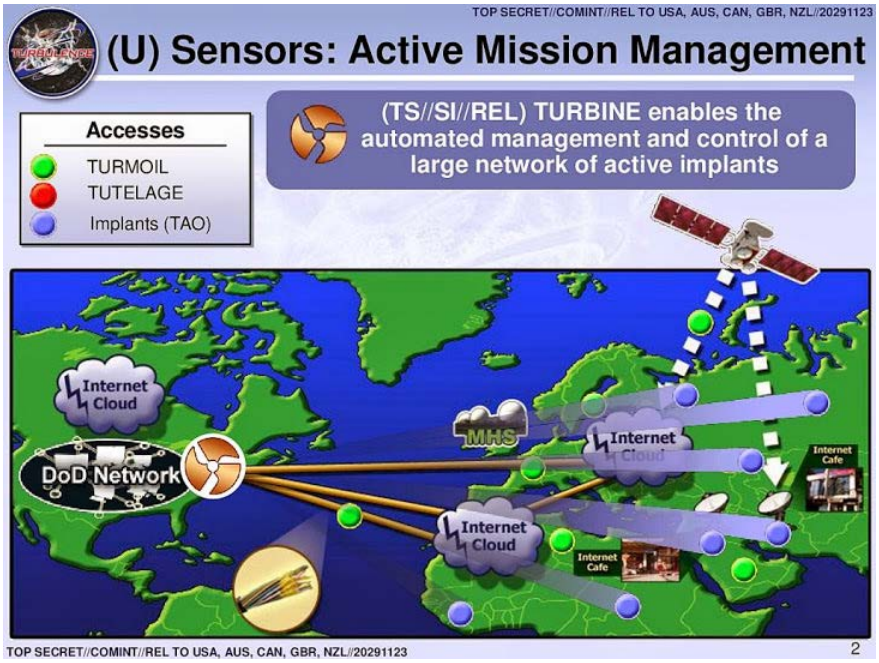
Ein Problem bei der typischen Virusverteilung bestand darin, dass es nach der Freisetzung eines Virus keine Möglichkeit gab, ihn zu kontrollieren. Die Idee eines zentralen Command & Control-Servers (C&C oder C2) löste dieses Problem und ermöglichte die

Verwaltung von Malware im aktiven Zustand.

Die Malware auf infizierten Computern, sogenannte Bots, blieb in Kontakt mit einem C&C-Server, der Befehle, Konfiguration und andere Anweisungen bereitstellte. Eine grosse Anzahl (Hunderte oder Tausende) infizierter PCs unter zentraler Kontrolle wird als botnet bezeichnet und kann von einer einzelnen Person, die als bot herder bezeichnet wird, ferngesteuert werden. Durch die Verwendung eines C&C konnte Malware auch mit neuen Versionen aktualisiert werden, die von Antivirenprogrammen weniger erkannt wurden.

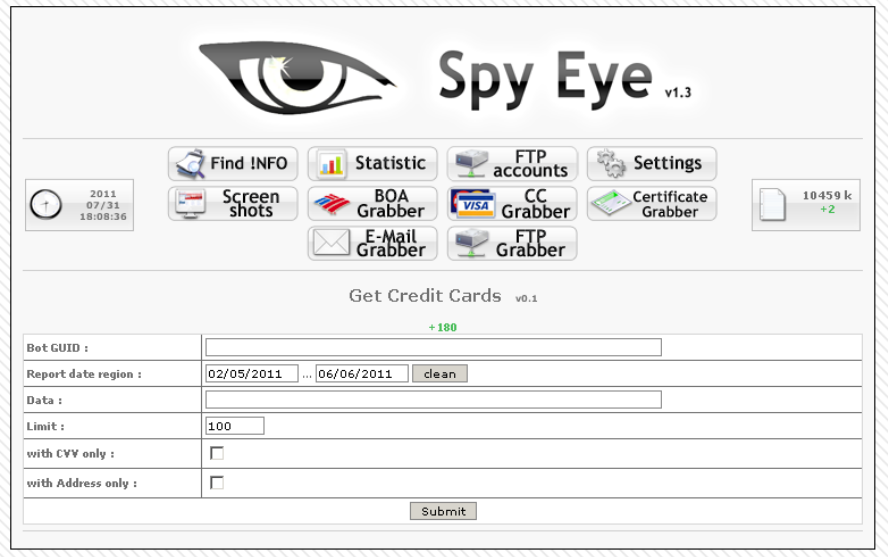
Die Botnetverwaltung war einfach und verwendete häufig komfortable Webschnittstellen. Das SpyEye-Botnet-Management-Panel ist ein gutes Beispiel dafür, wie ein Hacker Passwörter, Kreditkarten, E-Mails stehlen, Screenshots erstellen und andere Botnet-Wartungsaufgaben ausführen kann.

Mitte der 2000er Jahre interessierten sich kriminelle Banden für Malware, um Kreditkarten zu stehlen und auf Online-Bankkonten zuzugreifen. Organisierte kriminelle Banden würden Botnets erstellen oder mieten, die Web-Injects verwendeten, um den Browser eines Benutzers zu manipulieren, während sie in ihrer Bank angemeldet waren. Die Malware würde es Kriminellen ermöglichen, betrügerische Zahlungen zu leisten, ohne dass das Opfer dies bemerkt.



Lecks von Snowden zeigen die Verwendung von staatlich gesponserter Malware

Die Geheimdienste der Regierung hatten auch ein Interesse daran, Malware zum Zwecke der verdeckten Überwachung, des Diebstahls von Informationen oder der Verursachung von Störungen zu verwenden. Die Lecks von *Edward Snowden* im Jahr 2013 zeigen die Verwendung staatlich gesponserter Malware. Dies wird häufig als APT oder Advanced Persistent Threat bezeichnet. Die bekannteste staatlich geförderte Malware, die zur Störung verwendet wurde, war Stuxnet, das verdächtigt wurde, das iranische Atomprogramm beschädigt zu haben.

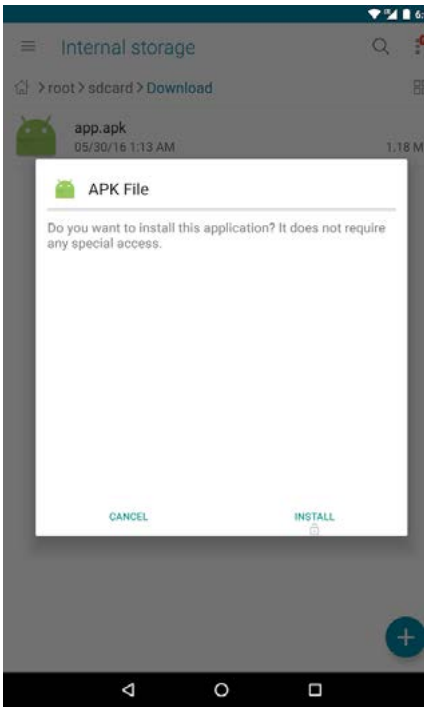


SpyEye Botnet Management Panel mit 10k bots 2011

Als Smartphones populär wurden, konzentrierten sich Kriminelle auf mobile Malware. Die meisten mobilen Malware-Programme wurden für Android geschrieben (Apple war schwieriger, da die Hardware, das Betriebssystem und die App-Stores strenger kontrolliert wurden). Beliebte mobile Malware verwendete einen Overlay-Angriff, der das Tippen mit dem Finger abfing und gefälschte Bildschirmaktivitäten präsentierte. Mobile Malware wurde verwendet, um Passwörter, PINs zu stehlen, SMS-Nachrichten abzufangen und vieles mehr.

Dies war besonders interessant für kriminelle Banden, die ver-

suchten, das MTAN für Bankanwendungen zu stehlen. Ein Telefon kann infiziert werden, indem dem Opfer ein Link zu einer APK gesendet wird, bei der es sich um ein Android-Softwarepaket handelt. Wenn der Benutzer der Installation zustimmt, wird das Telefon infiziert. Diese Techniken werden heute noch verwendet.



Google APK Install

Malware namens Ransomware verschlüsselt die Dateien eines Benutzers und verlangt dann, dass ein Lösegeld gezahlt wird (normalerweise heute in Bitcoin), um den Entschlüsselungsschlüssel zu erhalten. Kriminelle erwarteten, wenn der Benutzer keine Backups hatte und die Dateien wertvoll genug waren, würden sie bezahlen.

Einer der frühesten Ransomware-Viren war Ende der 1980er Jahre, der auf Diskette an AIDS-Forscher verteilt wurde. Der Virus verschlüsselte Dateien und verlangte eine Zahlung von 189 US-Dollar an ein Postfach in Panama. Der erste beliebte moderne Ransomware-Angriff war 2013 CryptoLocker.

Cryptolocker Ransomware

Es gibt so viele interessante und berühmte Viren, dass wir sie unmöglich alle beschreiben können. Zum Beispiel Brain, der ILOVEYOU-Virus, der Zeus-Banking-Trojaner, MyDoom, Nimda (Administrator rückwärts geschrieben), CodeRed und viele, viele andere.

Viren und Malware werden auch in Zukunft ein Problem bleiben. Noch heute sehen wir nicht nur Software-, sondern auch Hardware-Schwachstellen, die ausgenutzt werden können (z. B. Heartbleed und Spectre). Da die Hardware immer komplexer wird und sich schlecht gesicherte IoT-Geräte vermehren, werden in Zukunft mehr Formen von Malware erstellt.

Quellen:

Computer viruses: Theory and experiments, Fred Cohen Elsevier Computers & Security, Volume 6, Issue 1, February 1987 https://doi.org/10.1016/0167-4048(87)90122-2

The Internet Worm Program: An Analysis Eugene H. Spafford Purdue Technical Report CSD-TR-823, November 1988 https://spaf.cerias.purdue.edu/techreps/823.pdf

The Virus Information Summary List (VSUM): (Enthält 7 Viren, von denen vermutet wird, dass sie aus der Schweiz stammen) Patricia Hoffman http://wiw.org/~meta/vsum/

The Malware Museum: Mikko Hypponen http://archive.org/details/malwaremuseum&tab=collection

The History and Evolution of Computer Viruses Mikko Hypponen DEF CON 2011 https://youtu.be/yswPIwDFYDY

Der Artikel wurde von Florence Kunz übersetzt. Der englische Originalartikel befindet sich auf: https://digitalforensics.ch/nikkel20d.pdf

Original English version can be found here: https://digitalforensics.ch/nikkel20d.pdf